Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocols involved in this incident are **DNS**, **HTTP**, and **TCP**. • **DNS (Domain Name System)** was used to resolve the domain `yummyrecipesforme.com` into an IP address. • **HTTP (Hypertext Transfer Protocol)** was used to load the compromised website and deliver the malicious content. • **TCP (Transmission Control Protocol)** was the underlying transport protocol that enabled the reliable connection between the browser and the web server, allowing the HTTP traffic (including the malware redirect) to be successfully delivered.

Section 2: Document the incident
The attacker was a former employee who used a brute force attack to access the administrative panel of the `yummyrecipesforme.com` website by guessing the default password. Once logged in, the attacker modified the website's source code by injecting a malicious JavaScript function. When users visited the site, the JavaScript prompted them to download an executable file disguised as a browser update. After downloading and executing the file, users were redirected to a malicious website: `greatrecipesforme.com`. The sequence of events included:

- A DNS request to resolve `yummyrecipesforme.com`
- An HTTP request to the resolved IP address
- A manipulated HTTP response with malicious JavaScript
- A browser-initiated file download
- A redirection to a second malicious domain
- System slowdowns reported by users after running the file

The attacker also changed the admin password to retain control over the website and prevent administrators from stopping the attack.

Section 3: Recommend one remediation for brute force attacks

To prevent brute force attacks, the organization should implement **multi-factor authentication (MFA)** for all administrator accounts. MFA adds an extra layer of security by requiring users to verify their identity with something they know (a password) and something they have (such as a mobile app code or hardware token). Even if a password is guessed or stolen, unauthorized access is blocked without the second factor.

Additional recommendations include:

- Enforcing strong password policies (minimum length, complexity, and expiration)
- Limiting the number of failed login attempts before locking the account
- Disabling default usernames and passwords
- Logging and monitoring all login attempts for unusual behavior